



CVE-2002-0991

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

Summary

CVE	CVE-2002-0991
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2002-10-04 04:00:00 UTC
Updated	2008-09-05 20:29:00 UTC
Description	Buffer overflows in the cifslogin command for HP CIFS/9000 Client A.01.06 and earlier, based on the Sharity package, allow

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Hp	Cifs-9000 Server	a.01.05	All	All	All
Application	Hp	Cifs-9000 Server	a.01.06	All	All	All
Application	Hp	Cifs-9000 Server	a.01.05	All	All	All
Application	Hp	Cifs-9000 Server	a.01.06	All	All	All

References

Reference	
Neohapsis Archives - Bugtraq - Sharity Cifslogin Buffer Overflow (arguments) - From alex_hernandezureach.com	S
HP CIFSLogin Buffer Overflow Vulnerability	E
Neohapsis Archives - HP Security Digests - HP-UX security bulletins digest - From support_feedback_at_us-support-mail.external.hp.com	F
ISS X-Force Database: hp-cifs-login-bo (9431): HP CIFS/9000 /opt/cifsclient/bin/cifslogin buffer overflow	X
CVE Program record	C
NVD vulnerability detail	N

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)